20 Questions For Michael Chertoff

Rep. Bennie G. Thompson, Ranking Member
Committee on Homeland Security

February 2005

20 QUESTIONS FOR MICHAEL CHERTOFF

The confirmation hearings for Secretary of Homeland Security-designee Michael Chertoff mark an important moment in the mission to protect America. At this time of transition it is critical that we ask the right questions, set priorities, and develop strategies all with the singular purpose of ensuring that we do all we can to secure the homeland from the threat of terrorist attack.

The Department of Homeland Security has a mission vital to the very safety of our people and institutions. The U.S Congress has the responsibility to ensure the Department gets the job done right. For when it comes to protecting America, failure is not an option.

And so in carrying out the constitutional duty and the moral responsibility of doing all we can to provide for the common defense, the following twenty questions are put forward that go to the heart of answering the question - "are we doing all we can to make America safe from the threat of terrorist attack?"

Questions highlight the alarming security gaps that can be found in America's defenses on land, sea and air. Hard questions are asked about how prepared we truly are to meet the threat of biological terrorism, about the security of our critical infrastructure, and why it is that – after all the campaign talk and rhetoric – our first responders still do not have the tools they need to protect America's communities. The following questions are asked to satisfy our Constitutional responsibility of providing for the common defense – and answers are expected.

AVIATION: SECURING OUR SKIES

1: PASSENGER AND BAGGAGE SCREENING

We are spending nearly $5 billion each year on passenger and baggage screening systems, yet lethal weapons still are getting past security and onto planes. What changes will you make to make sure that weapons stay off passenger planes?

While we have devoted enormous attention and resources to improving aviation security, it is still far too easy for a terrorist to get a weapon on a passenger plane. The DHS Inspector General, the Government Accountability Office (GAO), and the Transportation Security Administration (TSA) all have conducted tests on TSA screeners at the nation's airports and found surprisingly high failure rates.[1] An alarming number of prohibited items are still not being detected during checks of passengers, carry-on items, and checked baggage. Clark Kent Ervin, the former DHS Inspector General, wrote in December that, "the department has been reluctant even to acknowledge the problem, much less put in place some of the recommendations that we made to fix it."[2]

2: AIR CARGO

While airline passengers may be screened, cargo beneath their feet is not. When will 100% of air cargo be screened?

The TSA has identified two critical risks to air cargo "(1) The hostile takeover of an all-cargo aircraft leading to its use as a weapon; and (2) the use of cargo to introduce an explosive device onboard a passenger aircraft in order to cause catastrophic damage."[3] Terrorists have exploited the lack of cargo security on several occasions. For example, a device in a baggage container of Pan Am Flight 103 caused the flight to explode in 1988 over Lockerbie, Scotland.[4] An explosion aboard a U.S. airliner in 1979 was caused by a parcel linked to the "Unabomber" Theodore Kaczynski and shipped as air cargo.[5] While Congress has mandated tripling air cargo screening, a large portion of commercial air cargo remain unscreened.[6] TSA relies heavily on the "Known Shipper" program, under which only approved companies may ship cargo on passenger aircraft. A company can become a "Known Shipper" with practically no security checks.

---

[1] Department of Homeland Security, *Audit of Passenger and Baggage Screening Procedures at Domestic Airports*, Office of Inspector General. September 2004

[2] Clark Kent Ervin, "Mission: Difficult, but Not Impossible," *The New York Times*, December 27, 2005, 17.

[3] Federal Register, Department of Homeland Security, Transportation Security Administration. Air Cargo Security Requirements; Proposed Rule. Vol. 69, No. 217, November 10, 2004. 65261

[4] See GAO, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO-03-344*, (Washington, D.C.: GAO, December 20, 2002), Appendix I: Air Cargo.

[5] Affidavit of Assistant Special Agent in Charge, Terry D. Turchie, before the U.S. District Court, District of Montana, April 3, 1996.

[6] "Homeland Security Appropriations Act for Fiscal Year 2005" (Public Law 108-334 §513).

RAIL SECURITY: KEEPING OUR TRAINS ON TRACK

3: RAIL SECURITY

America's passenger trains remain vulnerable – what will you do to prevent a Madrid-style bombing from happening during rush hour in an American city?

In March 2004, Al-Qaeda operatives attacked a commuter train in Madrid killing 200 people and wounding 1,500. In our own country, passenger rail and public transportation systems that carry million passengers a day remain vulnerable to terrorist attacks. While DHS has begun several rail and transit security initiatives such as research and development for explosive countermeasures, none of them will reduce the threat in the near-term. The GAO has stated that, "insufficient funding is the most significant challenge in making transit systems as safe and secure as possible**."**[7] Major rail and transit systems have estimated billions are needed to improve security for our passenger rail systems, yet DHS has put less than $300 million towards rail security over the last three years.[8] In addition, TSA has yet to take a leadership role in transit security. The roles of TSA and the Department of Transportation remain unclear and uncoordinated.

PORT SECURITY: PROTECTING OUR ECONOMY

4: PHYSICAL PROTECTIONS

When will you act to ensure owners and operators of port facilities receive the necessary support they need from the Department of Homeland Security to make urgently needed security improvements?

Ninety-five percent of the country's non-North America trade moves through America's seaports. [9] An attack on a port could result in substantial loss of life and economic damage ranging from $58 billion to $1 trillion.[10] To secure our seaports, the Coast Guard estimates that ports will have to spend $1.1 billion in initial costs and $5.4 billion over the next ten years.[11] Yet, the Administration has requested only $46 million since September 11th. While Congress has taken the lead and appropriated over $700 million, many ports cannot afford the security upgrades – such as lighting, fencing, surveillance systems – that this Administration is requiring them to install, thus leaving them vulnerable to attack.

---

[7] See GAO, *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*, GAO-03-263, (Washington, D.C.: GAO, December 2002), 2.

[8] Since fiscal year 2003, DHS' has provided a total of $227 million for rail security programs: $65 million in fiscal year 2003, $50 million in fiscal year 2004, and $150 million in fiscal year 2005 through the Office of Domestic Preparedness (ODP), and $12 million in fiscal year 2005 through TSA.

[9] Congressional Research Service, *Port and Maritime Security: Background Issues for Congress*, December 30, 2004. RL31733.

[10] $58 billion estimate is from the *Port Security Wargame-Implications from the Supply Chain*, Booz-Allen-Hamilton. February 2003. www.boozallenhamilton.com. $1 trillion comes from Michael O' Hanlon, *Protecting the American Homeland*, (Washington D.C.:The Brookings Institute Press 2002.)

[11] Federal Register Department of Homeland Security, U.S. Coast Guard. Facility Security Requirements; Final Rule. October 22, 2003. 60480.

5: RADIATION PORTAL MONITORS

When can Americans expect radiation portal monitors to be installed at all of our ports and border crossings to ensure that cargo is screened for weapons of mass destruction?

Secretary Tom Ridge once stated that "cargo security is a linchpin issue, not only for the security of our homeland, but also for our economic security as well."[12] Yet, millions of cargo containers are currently entering our ports without having been screened for nuclear and radiological materials. Overseas, few containers are actually inspected before they are shipped to the U.S. The vast majority of the foreign ports do not have adequate screening technology to detect a weapon of mass destruction hidden in a container. [13] The technology most frequently used by inspectors is hand held "radiation pagers," which is not an effective tool for comprehensive screening of cargo containers.[14] In fact the Department's Inspector General stated that detection equipment is one the areas where the Department needs to make improvements in order to ensure weapons of mass destruction or their components do not enter the country.[15]

6: PROJECT DEEPWATER

The plan to modernize the US Coast Guard is behind schedule and, at this rate, will not be completed until 2024. What will you do to speed the modernization of these frontline forces of the DHS?

The men and women of the U.S. Coast Guard are on the frontlines of the War on Terror. The increased operational tempo since 9/11 has further strained its aging fleet of cutters and aircraft. In fact a September 2004 report by the Inspector General stated that the "Coast Guard is experiencing serious cracking or breaches in the hulls of its 110 foot cutters and engine power losses on its HH-65 Dolphin helicopters."[16] The Coast Guard is in the process of replacing its assets through the Integrated Deepwater Systems programs. However, current funding levels would not allow the Coast Guard to complete the modernization of its fleet until 2024.

---

[12] Statement by Department of Homeland Security Secretary Tom Ridge to the Cargo Security Summit, December 16, 2004.

[13] Bureau of Customs and Border Protection Commissioner testified that five percent of containers are inspected. Testimony of Commissioner Robert Bonner before the National Commission on Terrorist Attacks Upon the United States. January 26, 2004. Democratic Staff trip to CSI ports December 13-17, 2004.

[14] Gary L. Jones, *Customs Service: Acquisition and Deployment of Radiation Detection Equipment.* U.S. General Accounting Office. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. October 17, 2002.

[15] Department of Homeland Security, *Effectiveness of Customs and Border Protection's Procedures to Detect Uranium In Two Smuggling Incidents*. OIG-04-40. September 2004 p 1.

[16] Department of Homeland Security, *FY2003 Mission Performance Unites States Coast Guard*, Office of the Inspector General OIG-04-43. September 2004 pp.16-18.

AGRO TERRORISM: SHIELDING OUR FOOD SUPPLY

7: AGRO TERRORISM

Given the security gaps that continue to exist regarding our nation's food supply – and in light of former Secretary Thompson's recent statements on the subject – what actions will you undertake immediately as the Secretary of Homeland Security to ensure that terrorists do not engage in acts of agro terrorism?

Recently, former Secretary for Health and Human Services Tommy Thompson stated that he worried "every single night" that someone would poison the nation's food supply.[17] Secretary Thompson went on to state that, "I, for the life of me, cannot understand why the terrorists have not…..attacked our food supply, because it is so easy to do. And we are importing a lot of food from the Middle East, and it would be easy to tamper with that." Although a biological attack against the nation's agricultural sector could result in a major public health crisis along with substantial economic and social disruptions, the United States is currently unprepared for such acts of "agro terrorism." DHS is assigned the task of analyzing foreign bioterrorism capabilities and is in the process of establishing a dedicated center to facilitate this effort – consistent with Homeland Security Presidential Directive 10 ("Biodefense for the 21st Century") – in addition to its border security responsibilities. It remains unclear, however, if it is currently capable of meaningfully contributing to the prevention of agro-terror.

CIVIL RIGHTS AND CIVIL LIBERTIES: PRESERVING OUR WAY OF LIFE

8: CIVIL RIGHTS AND CIVIL LIBERTIES

While you were the Assistant Attorney General for the Criminal Division at the Department of Justice, significant questions arose about the procedures you put in place regarding the detention of more than 700 Arab and South Asian men who were held without charges or access to lawyers for alleged immigration violations. What steps will you take to ensure that the Department of Homeland Security does not repeat the mistakes of the Department of Justice and unduly violate the civil liberties and Constitutional rights enjoyed by Americans?

According to a 2003 report by Justice Department Inspector General Glenn Fine, the Department of Justice, with guidance from Mr. Chertoff's Criminal Division, detained more than 700 Arab and South Asian men for immigration violations, holding them without charges or access to lawyers for an average of three months. Not one of these individuals was charged with any crime.[18] This was done even though immigration rules entitle detainees to the right of counsel.

[17] "The Nation; Bush Downplays Warning on Food Supply," *Washington Post* (Reuters), December 5, 2004, A27.
[18] Michael Powell & Michelle Garcia, Amid Praise, Doubts About Nominee's Post-9/11 Role, *Washington Post*, January 31, 2005.

BORDER SECURITY: DEFENDING OUR BORDERS

9*:* US-VISIT

Will you direct that DHS comply with past Congressional mandates and give local, state and federal law enforcement agencies the same access to search the US-VISIT database that they presently have to search numerous other government databases?

Both the 2001 USA Patriot Act and the 2002 Enhanced Border Security and Visa Reform Act mandated the development of an integrated system for sharing law enforcement and intelligence information about people entering the United States.[19] In response, DHS created the United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT), a complex, multi-year project designed to manage the pre-entry, entry, and exit of foreign nationals who travel to the United States. According to a new report by the Department of Justice (DOJ) Office of Inspector General, US-VISIT is not being developed to share information readily. The Inspector General reported that, "DHS disagrees with the (the Department of Justice) that a fully interoperable system must provide federal, state, and local law enforcement agencies with ready access to … immigration records." This lack of information sharing means that a terrorist could enter the country undetected.[20]

10: BORDER SECURITY RESPONSIBILITIES

What steps will you take to consolidate border security responsibilities to ensure that frontline officers responsible for border, immigration, and transportation security are all talking to one another? Will you consolidate Customs and Border Protection with Immigration and Customs Enforcement?

According to a recent report by the Heritage Foundation and the Center for Strategic and International Studies, DHS – in "consolidating" responsibility for border, immigration, and transportation security – actually increased the number of agencies involved in securing our borders from seven to eight.[21] In addressing border security, the Department split up the departments of Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE), having the first focus on "border enforcement" and the latter on "interior enforcement." The result, however, has been a disjointed approach to border security that leaves our borders at risk.

---

[19] *USA-PATRIOT Act* (P.L. 107-56), Section 403 (c) (2); *Enhanced Border Security and Visa Reform Act of 2002* (P.L. 107-173 Section 202 (a) (4) (B)

[20] Follow-up Review of the Status of IDENT/IAFIS Integration Report Number I-2005-001 (Page iv).

[21] James Jay Carafano, and David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security DHS 2.0* (Washington, D.C.: The Heritage Foundation and the Center for Strategic and International Studies, December 13, 2004) p. 15.

11: IMMIGRATION AND CUSTOMS ENFORCEMENT SHORTFALLS

What will you do to ensure that ICE is properly funded and no longer facing shortfalls?

ICE is the DHS component responsible for enforcing our nation's immigration and customs laws and securing our federal buildings and airline flights. Since DHS was created, ICE has faced crippling financial shortfalls that have forced widespread hiring freezes and a 45 percent cut in most operating expenses, such as travel, equipment purchases, and employee training.[22] Many experts have questioned the effectiveness of the Federal Financial Management System to accurately keep track of ICE's budget. The deficiencies in ICE's use of the system have been so severe that ICE is in danger of violating the Anti-Deficiency Act, a key federal law which restricts agencies from over-obligating appropriated funds.[23]

FIRST RESPONDERS: PREPARING OUR COMMUNITIES

12*:* FIRST RESPONDER CAPABILITIES

When will the Department establish standards and provide the resources necessary to ensure that every American community has the capability to respond in case of a terrorist attack?

In December 2002, the Gilmore Commission stated that, "without a comprehensive approach to measuring how well we are doing with the resources being applied at any point in time, there will be very little prospect for answering the question 'How well prepared are we?'"[24] As the Council of Foreign Relations found in 2003 – we are not prepared. There is "currently an inadequate process for determining, and therefore addressing, America's most critical needs. America's leaders have not yet defined national standards of preparedness—the essential capabilities that every jurisdiction of a particular size should have or have immediate access to."[25] Without such standards and guidelines, such as technical specifications for equipment and minimum training standards, both state and local governments and first responders lack sufficient information to determine their preparedness needs and the costs of these needs. Additionally, without such preparedness standards, is it unclear what basis DHS has for its budget requests for first responder grant programs.

[22] Letter to Secretary Tom Ridge from Rep. Martin Sabo, Ranking Member, House Appropriations Subcommittee on Homeland Security, November 19, 2004.
[23] Letter to former DHS Inspector General Clark Kent Ervin from former Rep. Jim Turner, Ranking Member, Select Committee on Homeland Security, June 14, 2004.
[24] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fourth Annual Report to the President and the Congress*, Rand (December 2002), 37.
[25] Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, June 2003), 7.

13: INTEROPERABLE FIRST RESPONDER COMMUNICATIONS

More than three years after the attacks of September 11th, our first responders still are not guaranteed equipment so that they can talk to one another at a disaster scene. What immediate steps will you take to make communications interoperable and by what date will you close this security gap that threatens the lives of first responders?

The public hearings of the 9/11 Commission revealed that effective decision-making and emergency response in New York were prevented by limited command and control and internal communications, and that at the Pentagon, "Almost all aspects of communications continue[d] to be problematic."[26] The Council on Foreign Relations has reported that, in virtually every major city and county in the United States, no interoperable communications system exists to support police, fire departments, and response personnel at all levels of government during a major emergency,[27] and that a minimum, $6.8 billion over five years would be necessary to ensure dependable, interoperable communications for first responders.[28] On at least two occasions during 2004, Secretary Ridge publicly identified the enhancement of communications interoperability as a priority issue for DHS.[29] Yet, the Administration requested no dedicated funds for current year grants to state and local governments to improve interoperability. At the same time, the principal existing Federal program to address interoperable communications—the Wireless Public Safety Interoperable Communications program (Project SAFECOM)—has made very little progress, principally due to a lack of consistent executive commitment and support, and an inadequate level of interagency collaboration.[30]

---

[26] National Commission on Terrorist Attacks upon the United States, *Staff Statement No. 14, Crisis Management* (Washington: National Commission on Terrorist Attacks Upon the United States, May 19, 2004), 8-10.
[27] Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, America Still Unprepared, America Still in Danger* (New York: Council on Foreign Relations, 2002), 14.
[28] Council on Foreign Relations, *Report of an Independent Task Force Sponsored by the Council on Foreign Relations, Emergency Responders: Drastically Underfunded, Dangerously Unprepared* (New York: Council on Foreign Relations, June 2003), 33.
[29] (a) Statement by Secretary Tom Ridge on the One-Year Anniversary of the Department of Homeland Security, *ONLINE* (February 23, 2004), http://www.dhs.gov/dhspublic/display?content=3204 [June 9, 2004]; (b) Written Testimony of Secretary Tom Ridge, U.S. Department Of Homeland Security, to the National Commission on Terrorist Attacks Upon the United States, (Washington: Department of Homeland Security, May 19, 2004), 9-10.
[30] GAO, *Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration, GAO-04-494* (Washington, D.C.: GAO April 2004).

CRITICAL INFRASTRUCTURE PROTECTION: SAFEGUARDING OUR NATION'S ASSETS

14*:* ASSESSING CRITICAL INFRASTRUCTURE AND ASSETS

Three and a half years after 9-11 we lack a list that tells us where we are most vulnerable so that we might be able to protect ourselves from terrorist attack. At the same time, the government's plan for protecting critical infrastructure is long overdue. When will the nation's critical assets be catalogued and when will the National Critical Infrastructure Protection plan be released?

The Homeland Security Act requires DHS to assess and provide for the protection of our nation's critical infrastructure in sectors such as telecommunications, energy, and food and water. Homeland Security Presidential Directive 7, released in late 2003 by President Bush, calls for the creation of a National Critical Infrastructure Plan – which was due December 17, 2004. [31] However, as of today, it has not been released. In addition, Secretary Tom Ridge promised in February 2004 that the creation of a national asset database of potential terrorist targets would be completed by the end of 2004.[32] Like the National Plan, the asset database is far behind schedule.[33] According to Secretary Ridge in a July internal memo, local officials lack "clear guidelines and standards" from DHS to help them determine which sites to include. He went on to write, "Absent such clear delineation, it is impossible to justify any item contained on the national list." [34]

15: CHEMICAL SECURITY

Millions of Americans live in the shadow of highly vulnerable chemical plants. What specific steps will you take to ensure that these facilities will be secure from terrorist attack?

The U.S. is home to more than 66,000 chemical production and storage facilities throughout its cities, towns, and rural areas. These sites are unprotected and at risk. In November 2003, the television magazine *60 Minutes* reported unlocked gates, absent guards, dilapidated fences, and unprotected tanks filled with deadly chemicals at dozens of facilities in major metropolitan areas.[35] In the Pittsburgh area, one reporter found easy access to more than 200 tons of corrosive chlorine gas at four different sites.[36] The GAO has twice reported that no comprehensive assessment of the vulnerability of or the security at chemical facilities has been completed, and no agency monitors, documents, or sets standards for the implementation of chemical security measures by industry.[37]

---

[31] Homeland Security Presidential Directive/Hspd-7 Critical Infrastructure Identification, Prioritization, and Protection, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[32] Statement by Secretary Ridge on the One-Year Anniversary of the Department of Homeland Security, George Washington University, Homeland Security Policy Institute, February 23, 2004.

[33] "Terror Target List Way Behind," *USA Today*, December 2004.

[34] Id.

[35] U.S. Plants: Open for Terrorists," *60 Minutes*, broadcast November 16, 2003.

[36] Carl Prine, "Chemical Sites Still Vulnerable," Pittsburgh Tribune-Review, November 16, 2003.

[37] GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439 (Washington, D.C.: GAO March 2003); GAO, *Homeland Security:*

16: CYBERSECURITY

Will you create an Assistant Secretary for cybersecurity, to work side-by-side with the country's physical infrastructure assistant secretary, within the Information Analysis and Infrastructure Protection Directorate? When will America see definitive actions on the National Strategy to Secure Cyberspace?

The federal government is not adequately prepared to fend of a cyberattack that could devastate our economy and infrastructures. In addition, our nation risks the possibility that a terrorist could use a cyberattack in connection with a physical attack, cutting off vital infrastructures and communications. Despite these threats, the highest cybersecurity official in the government has been demoted from a Presidential special assistant to a director buried four layers into DHS' bureaucracy. The President's *National Strategy to Secure Cyberspace*, released in February 2003, remains unimplemented. The result of this lack of attention, according to the Department's own Inspector General, is that our nation's efforts to battle cyberattacks suffer from a lack of coordination, poor communication, and an inability to set priorities.[38] In early December, 2004, several executives in the technology industry called on the Administration to strengthen cyber infrastructure and protect end users from cyberattacks.[39]

INTELLIGENCE: PREVENTING ANOTHER 9-11

17: INTELLIGENCE MISSION

What will be done to ensure that the Department has access to all the intelligence it needs to prevent terrorist attacks and fulfill its mission?

The Homeland Security Act, on paper, makes the Department of Homeland Security (DHS) a major player in the intelligence community, with responsibilities for establishing intelligence collection priorities, analyzing terrorism intelligence, and ensuring that information sharing problems that occurred before 9/11 would no longer happen. Since the Act was passed, the President created the Terrorist Threat Integration Center (TTIC) under the Director of the Central Intelligence and the Terrorist Screening Center under the Federal Bureau of Investigation (FBI). Last year, Congress created the position of National Intelligence Director and the National Counter Terrorism Center to replace the TTIC. All of these new entities take part of the jurisdiction originally assigned to DHS. According to the Department's former Inspector General, "the Department's information analysis unit was crippled almost from the start."[40]

Federal Action Needed to Address Security Challenges at Chemical Facilities, GAO-04-482T (Washington D.C.: GAO February 2004).

[38] Department of Homeland Security, *Progress and Challenges in Securing the Nation's Cyberspace*, Office of Inspector General OIG-04-29 (July 2004).

[39] *See* https://www.csialliance.org/resources/pdfs/Agenda_for_Next_Administration.pdf

[40] Clark Kent Ervin, "Mission: Difficult, but Not Impossible," *The New York Times*, December 27, 2005, 17.

18: INFORMATION SHARING

How will you fix the broken system that is keeping our federal, state, and local officials from effectively sharing information about terrorist threats?

There is almost universal agreement that the failure to share information among federal, state, and local governments contributed to the success of the 9-11 attacks.[41] Little has improved since the attacks. This past December, the Department's own Advisory Council reported that federal information sharing was not meeting the needs of state and local partners in securing the homeland.[42] This is troubling because the Department is responsible coordinating "appropriate exchanges of information, including law-enforcement information, relating to threats of terrorism against the United States."[43] Today, the FBI continues to disseminate threat information relevant to homeland security to law enforcement officials through its Joint Terrorism Task Forces, creating a duplicative and sometimes conflicting information sharing system.

INTERNATIONAL RELATIONS: REACHING BEYOND AMERICA

19: INTERNATIONAL ACTIVITIES

W*hat actions will you take immediately to strengthen the Department's organization and management of its international offices?*

The Heritage Foundation and the Center for Strategic and International Studies recently released a report addressing DHS' international operations involving diplomatic intelligence, information sharing, and other cooperative activities within foreign countries. The report found that the Department's efforts remain fragmented among multiple offices. According to the report:

> Because of this fragmentation (which reflects DHS's overall incomplete integration), DHS is unable to present a unified effort and presence overseas. As a result, DHS remains disenfranchised from the foreign policy apparatus. Within embassies, DHS presence is ad hoc and its role, mission, and relationship with the rest of the embassy are unclear. Foreign governments that share security interests with the U.S. may fail to build effective partnerships because of the lack of a clear path to partnership. DHS is poorly represented among important international organizations, including the European Union and the Organization for Security and Cooperation in Europe, which could play extremely helpful roles in homeland security.[44]

---

[41] See, for example, House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, *Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001*, House Report 107-792 and Senate Report 107-351, December, 2002; and National Commission on Terrorist Attacks upon the United States, (Washington: National Commission on Terrorist Attacks Upon the United States, 2004).

[42] Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative." December, 2004. Available online at http://www.dhs.gov/interweb/assetlibrary/HSAC_IntelInfoSharingReport_1204.pdf.

[43] "Homeland Security Act of 2002" (Public Law 107-296 §201(d)(11)).

[44] James Jay Carafano and David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, the Heritage Foundation and the Center for Strategic and International Studies. December 13, 2004, 13.

RESEARCH & DEVELOPMENT: PLANNING FOR THE FUTURE

20: SCIENCE AND TECHNOLOGY INTEGRATION

If confirmed, will you order the consolidation of research work and move the R&D budget functions from Department agencies to the Science and Technology Directorate?

There has been little progress on the consolidation of research and development activities within the Department. Plans to move research and development from legacy agencies into the Science and Technology Directorate have been languishing on Secretary Ridge's desk for months. For example, science and technology-related work at the Transportation Security Administration, the US VISIT program, the Secret Service, the Bureau for Immigration and Customs Enforcement, and the Coast Guard remains uncoordinated.